



Het einde van de firewall nabij?

Bij het beveiligen van onze informatie speelt het concept van perimeterbeveiliging nog altijd een grote rol. Dit houdt in dat er om informatieverwerkende systemen een grens wordt getrokken.

Vervolgens wordt er een muur om de grens gezet.

Informatiebeveiliging binnen organisaties is nog altijd gebaseerd op dit concept. Er wordt een hoge muur om de organisatie getrokken. Vervolgens laten we zeer beperkt en gecontroleerd verkeer toe tussen de onveilige buitenkant en de veilige binnenkant.

Uiteraard wordt er binnen de organisatie nog de nodige aanvullende maatregelen getroffen, zodat we niet alleen afhankelijk zijn van onze perimeterbeveiliging. Zo wordt ondermeer compartimentering toegepast (wat feitelijk een extensie is op het perimeter concept), zodat een doorbraak van de perimeter niet automatisch leidt tot toegang tot alle systemen.

Het bovengenoemde concept is gebaseerd op de aanname dat er slechts beperkte interactie is met de buitenwereld. Dit ging tot een aantal jaren terug voor veel organisaties nog op. Bedrijfsinformatie blijft echter niet meer alleen binnen de veilige muren van de organisatie. Medewerkers werken thuis. Er wordt informatie uitgewisseld met externe partijen. IT-diensten worden uitbesteed. Klanten hebben online toegang tot hun gegevens. Informatie wordt meer en meer uitgewisseld met externe partijen.

Door deze ontwikkelingen heeft perimeterbeveiliging zijn kracht verloren. Er moeten vele gaten worden gemaakt in de perimeter om te kunnen voldoen aan de eisen vanuit de organisatie.

Vaak wringen beveiligers en IT-specialisten zich in allerlei bochten om de benodigde gaten zo klein mogelijk te houden of verbieden eenvoudig het maken van gaten. Het krampachtig vasthouden aan de perimeterbeveiliging is echter geen optie. Het frustreert de business en is ineffectief.

Bovendien is de informatie, indien eenmaal buiten de perimeter, onbeschermd. Veel informatie staat bij partners, klanten of bij medewerkers thuis op een PC of USB stick.

Door deze ontwikkelingen is er de noodzaak om een ander beveiligingsconcept te kiezen, waarbij de beveiliging "dichter" bij de informatie zelf zit.

Op dit punt is er een aantal ontwikkelingen. Zo is er het Jericho Forum. Dit forum heeft een visie ontwikkeld die déperimeterisation wordt genoemd. Daarnaast is een aantal concepten uitgewerkt. Hieronder wordt een tweetal concepten genoemd:

Het concept van het plaatsen van standaard security services buiten de deur: WEB filtering, Email filtering vindt niet langer binnen het bedrijfsnetwerk plaats maar via een speciale provider. Hierdoor kunnen medewerkers buiten het bedrijfsnetwerk of partners ook gebruik maken van deze services. Het concept van de beveiliging op dataniveau. Dit houdt in dat toegang tot een databestand altijd wordt gecontroleerd langs de autorisatieregels die voor dat bestand gelden, ongeacht of dit bestand is gekopieerd of getransporteerd via email, USB stick etc. Dit impliceert een "schil" om het databestand heen die toegang controleert.

Deperimeterisering is uit het ideeënstadium gekomen en de verwachting is dat binnen een aantal jaren er toepassingen zullen zijn.

Bronnen:

<http://www.opengroup.org/jericho/>

<http://www.zdnet.nl/print.cfm?id=74825>

Secure Connection is verhuisd

Secure Connection heeft vanaf 1 oktober 2007 een nieuwe locatie. Hieronder vindt u de adresgegevens:

Secure Connection BV

Smederijstraat 2

4814 DB Breda

Postbus 3196

4800 DD Breda

Tel: 076 - 531 7731

Fax: 076 - 531 7701

<http://www.assutools.com>

Actueel

Default wachtwoorden

Nog steeds worden default wachtwoorden op routers en firewalls thuis niet gewijzigd en is het default wachtwoord geldig.

Nu is het zo dat de meeste routers/firewalls default de toegang tot de router/firewall van buiten af dicht zetten. Dit lijkt misschien veilig, maar dat is het niet.

Er zijn stukjes javacode ontwikkeld die vanaf uw PC thuis toegang proberen te krijgen tot uw router/firewall.

Als dit succesvol is, wordt vervolgens de router/firewall open gezet voor toegang van buitenaf. Nu kan een aanvalleur eenvoudig toegang krijgen tot uw thuisnetwerk.

Deze techniek wordt cross-site request forgery genoemd. Meer hierover is op onze site te vinden.

Er is op dit moment een database van default wachtwoorden te vinden op het internet. Mocht u niet meer weten wat uw default wachtwoord is, dan kunt u dit gewoon vinden in deze database (zie onderstaande link).

Advies: wijzig vandaag nog uw default wachtwoord!

Bron:

(database)

<http://www.routerpasswords.com/>

(cross site request forgery)

<http://www.assutools.com/news/strategies/>